

APPLICANT(S): Elad Barkan
SERIAL NO.: 10/046,745
FILED: January 17, 2002

Page 2

REMARKS

The present response is intended to be fully responsive to all points of objections and/or rejections raised by the Examiner and are believed to place the application in condition for allowance. Favorable reconsideration and allowance of the application is respectfully requested.

Applicant assert that the present invention is new, non-obvious and useful. Prompt consideration and allowance of the claims is respectfully requested.

Status of Claims

Claims 14 through 28 are pending in the application.

35 U.S.C. § 102 Rejections

On Pages 2-3 of the Office Action, in Paragraphs 3-10 the Examiner has rejected claims 14-19,21-24,26 under 35 U.S.C. §102(b) as being anticipated by Micali, US Patent No. 5,604,804 ("Micali").

Micali discloses a method for certifying public keys in a digital signature scheme. Conversely independent claims 14 & 22 clearly recite the limitation of authorizing an electronic device to act as a representative of a CA. **Micali** does not disclose, teach or suggest this limitation. Implementing in an electronic device a document issuing policy that enables the device to act as a representative of the CA is not suggested, taught or disclosed by **Micali**. As well established under U.S. patent law, for a reference to anticipate a claim, the reference must teach all elements of the claim.

Regarding Paragraph 5 of the office action, Examiner alleges that Micali **"discloses the implementing in device a document issuing policy of the CA see Col 2 Ln 17-31 ;"**. Applicants fail to see how the cited paragraph is relevant to the implementing in device a document issuing method of a certifying authority (CA). For example, the cited paragraph disclose the need of accountability of intermediate authorities **"if a user presents an intermediate authority with a piece of data to be certified, such as public key, and the intermediate authority individually certifies the data and passes this certification on to a higher authority who issues the certificate, the intermediate authority should not be able to latter deny having contributed to the certification of the piece of data"**. Nowhere in the referred paragraph *implementing in device a document issuing policy of the CA* is disclosed, taught or suggested.

The examiner also alleges that Micali discloses *"reading into device a certified document associated with user see Col 3 Ln 13 – 28"*. Applicants fail to see how the cited paragraph is relevant to the reading into device a certified document associated with user. According to Micali in the cited paragraph : ***"The piece of data that is presented may be a public key having at east one corresponding secret key. A user may choose the public key to be used in connection with either a digital signature system or a public key encryption system"***. Therefore, It is clear that the user chooses the piece of data to be certified. In distinction to Micali in the present invention a certified document (that already has been issued by a CA) is read into the device.

The examiner also alleges that Micali discloses *"generating of behalf of CA a new certified document based on read document see Col 6 Ln 14-26"*. Applicant fail to see how the cited paragraph is relevant to generating on behalf of the CA a new certified digital document based on the read certified digital document and issuing policy. For example it is disclosed in the cited paragraph that the issuing authority can add information to its own issuing certificate to prove the accountability of intermediate authorities that contributed to the certification: ***"The issuing authority may cause additional information to be saved which, when combined with the information that is stored, proves that the intermediate authorities contributed to***

certification of the piece of data." And so on. Nowhere in the referred paragraph, a device generating on behalf of a CA a new certificate based on a read certified document and an issuing policy previously implemented in the device, is disclosed taught or suggested.

Regarding Paragraph 6 of the office action, Examiner alleges that Micali ***"discloses the identity of device in form of digital signature stored with intermediate CA see Col 4 Ln 18-42."*** Applicants fail to see how the cited paragraph is relevant for storing the identity of the device or its user within the electronic device. For example the cited paragraph discloses that additional identifying information of an intermediate authority can be saved and added to the signature of another authority in order to prove that the intermediate authority contributed to the certificate to be issued: ***"The portion of the digital signature may be combined to prove that Aj contributed to the certificate being issued"***. Nowhere in the referred paragraph information associated with the identity of the electronic device itself or its user is disclosed, taught or suggested.

Regarding Paragraph 7 of the office action, Examiner alleges that Micali ***"discloses the policy attests to personal identifying information of user see Col 6 Ln 28-39"***. Applicants fail to see how the cited paragraph is relevant to the issuing policy attesting personal identifying information of the user. For example, in the cited Paragraph Micali disclose that information that is stored can be stored in a way to prove in the future the identity of a witness: ***"The portion of the digital signature can be combined to prove that the intermediate authorities contributed to certification of the piece of data"***. Nowhere in the referred paragraph a certificate issuing policy that attests the user personal identifying information is disclosed, taught or suggested.

Regarding Paragraph 8 of the office action, Examiner alleges that Micali ***"discloses the certified document being output thorough a secure channel see Col 5 Ln 20-36"***. In the cited paragraph Micali discloses the need to limit or save certificate size in a communication systems ***"Such transmission and storage costs, however, are incurred..."***. Applicants Claim 17 is dependent on Claim 14, and allows the method

of Claim 14 to be output through a communication channel. Therefore this claim 17 should be allowed in conjunction with Claim 14

Regarding Paragraph 9 of the office action, Examiner alleges that Micali **"discloses the digital documents being certificates and permits see Col 5 Ln-37-45"** Applicants read carefully the cited paragraph of Micali and failed to see any disclosure, teaching or suggestion by Micali that documents might or could be permits. Furthermore, Claim 18 is dependent on Claim 14, and allows the method of Claim 14 to be output as a permit or certificate. Therefore this claim 17 should be allowed in conjunction with Claim 14

Regarding Paragraph 10 of the office action, Examiner alleges that Micali **"discloses the signing of certificates and authorities along the path see Col 6 Ln 14-26"**. Applicants fail to see the relevance of the cited paragraph to Claim 19, and 21,26. For example In the cited Paragraph Micali discloses that certificate issuing authorities can include additional information to their issued certificates: **"The issuing authority may cause additional information to be saved which, when combined with the information that is stored, proves that the intermediate authorities contributed to certification of the piece of data."** . In distinct to Micali, Claim 19 of the present invention claims that identification of a user by the device is being performed prior to the action of the device to sign or certify a digital document. Furthermore, Claims 21 and 26 of the present invention claim that a **"plurality of certified digital documents associated with the user is stored within the electronic device...each of which is associated with a different certifying authority"**. Nowhere in the cited paragraph the identification of a user to the device prior to the device signs or certifies a digital document, nor the storing of a plurality of certified digital document in a device is disclosed, taught or suggested.

According to Micali **"According to the present invention, certifying pieces of data in a system with at least two levels of authorities includes presenting a piece of data requiring certification to a first level authority causing a higher authority to receive an indication having the higher authority issue a certificate that the piece of data possesses the given property.... And storing information in order to**

keep at least the first level authority accountable..." (Col. 2 Line 57 – Col. 3 Line 3). It is clear that Micali discloses a mechanism that involves at least two levels of authorities, to store information in a certificate and to keep an intermediate level authority accountable for the issuing of the certificate by a higher authority, rather than implementing in device a document issuing policy of the CA, as disclosed in the present invention.

In distinction to Micali, the present invention discloses a method to authorize an electronic device ("smart card") to act as a representative of the CA itself, without the need of an intermediate authority ("*This method, in fact, transform the smart card into a subcontractor of that known Certifying Authority (CA), for the purpose of issuing permits or certificates. Thus, the smart card now can issue permits or certificates on behalf of the original CA authority.*", Page 3, pars. 84-85.).

Making a smart card a representative of a CA eliminates the need for making intermediate authorities accountable for signing or certifying, because the smart card acts as the CA itself ("*..., the device will operate as a certified authority according to the program or document issuing method that originates with the known authority*", Page 9 par. 279). This means that the (genuine) CA is replaced (represented) by the smart card.

35 U.S.C. § 103 Rejections

On Pages 4-5 of the Office Action, in Paragraphs 11-15 the Examiner has rejected claims 20 and 25 under 35 U.S.C. §103(a) as being anticipated by Micali, US Patent No. 5,604,804 ("Micali") in view of US Patent No. 5,872,848 ("Romney").

Regarding Paragraphs 12 and 13 of the Office Action, **Romney** discloses a method and apparatus for witnessed authentication of electronic documents. In view of the foregoing remarks to 35 U.S.C. § 103 examiner rejections, independent claims 14 & 22 are considered allowable, as they were not disclosed, taught or suggested neither by Micali nor by Romney. Furthermore, Claim 20 is dependent on Claim 14,

APPLICANT(S): Elad Barkan
SERIAL NO.: 10/046,745
FILED: January 17, 2002

Page 7

and Claim 25 is dependent on Claim 24 which in turn is dependent on Claim 22. Therefore, Claims 20 and 25 should be allowed, as they add the biometric additional identification to the independent Claims 14 and 22 respectfully.

Regarding Paragraphs 14 and 15 of the Office Action, **Deo** discloses an authentication system and method for smart card transactions. In view of the foregoing remarks to 35 U.S.C. § 103 examiner rejections, independent claim 22 is considered allowable, as it was not disclosed, taught or suggested neither by Micali nor by Deo. Furthermore, Claim 27 is dependent on Claim 22 and in that scope adds the claim that the device of Claim 22 is functionally associated with a wristwatch.

Claim 28 is dependent on Claim 22. In that scope it adds the claim that the device of Claim 22 is functionally associated with a smart card. Therefore, the disclosure of Dio in conjunction with Micali does not affect the allowability of the device of Claim 22. Dio's disclosure of wristwatch is not related at all to the device of Claim 22 and was not cited against this Claim 22. Therefore it is not obvious to have the device of Claim 22 to be implemented in a wristwatch or a smart card. Accordingly, Claims 27 and 28 are not obvious and should be allowed.

In view of the foregoing remarks, the all pending claims 14 through 28 are considered allowable. Their allowance is respectfully requested.

Respectfully submitted,



Elad Barkan

12 Habanin Street,
Kefar Sirkin 49935,
ISRAEL

Email: moti@barkan.org